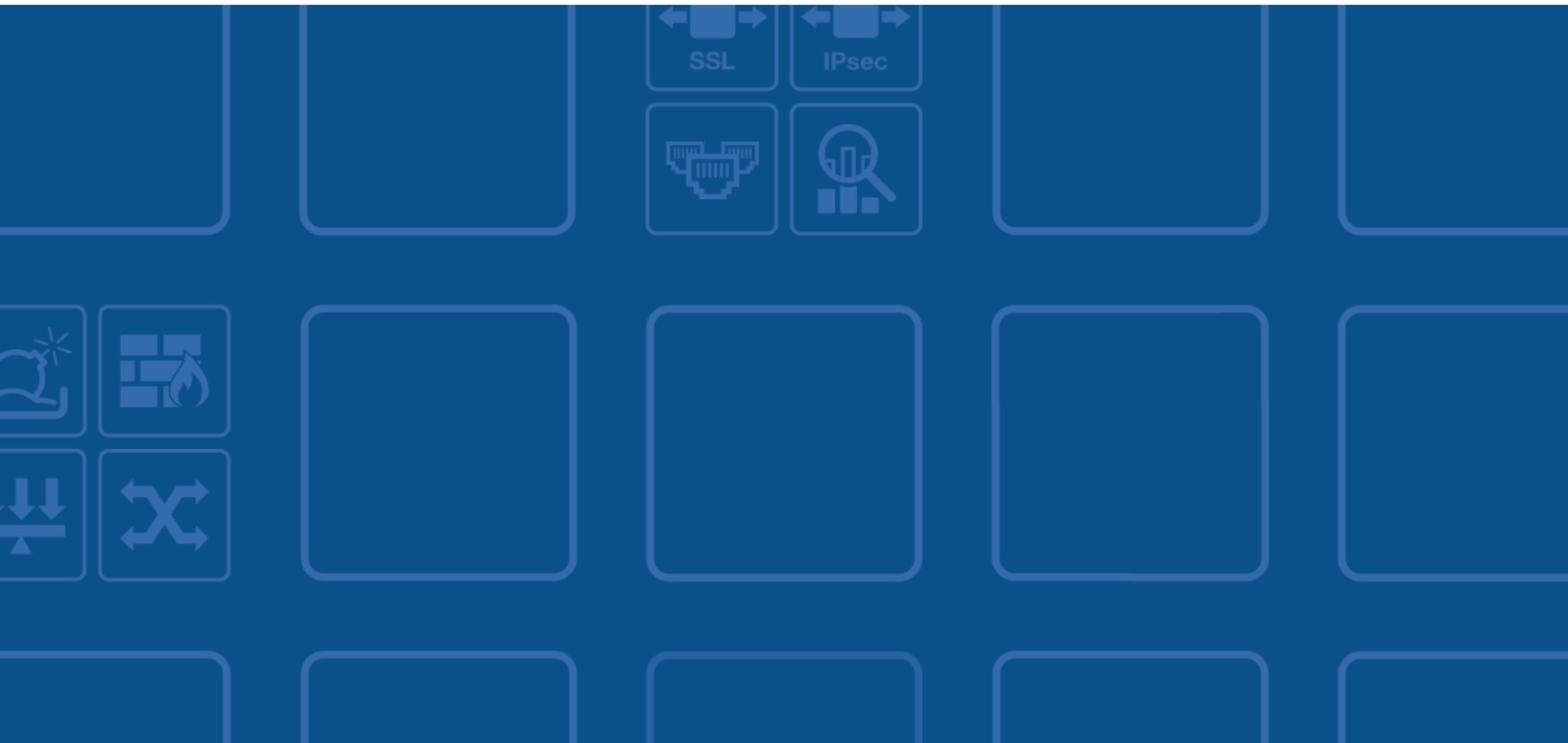
FORTINET
High Performance Network Security

FortiClient EMS - Release Notes

VERSION 1.0.1



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 05, 2016

FortiClient EMS 1.0.1 Release Notes

04-101-357361-20160705

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-06-24	Initial release.
2016-07-05	Updated *Endpoint Requirements* information.

Introduction

FortiClient Enterprise Management Server (EMS) is a system intended to be used to manage installations of FortiClient. It uses the same Endpoint Control protocol that was introduced in FortiOS 5.0 and enhanced in FortiOS 5.2. Like FortiOS, EMS supports all FortiClient platforms: Microsoft Windows, Mac OS X, Android OS and Apple iOS. FortiClient EMS does not require a Fortinet device. It runs on a Microsoft Windows server. End users with FortiClient installations could choose to use a FortiGate or the EMS to manage their installations.

This document provides the following information for FortiClient EMS 1.0.1 build 0077:

For more information about FortiClient EMS, see the *FortiClient EMS Administration Guide*.

Supported platforms

The EMS server can be installed on any of the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2

System Requirements

The minimum system requirement is as follows.

- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 8 GB RAM
- 20 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

See also the subsection: Management Capacity in the Main Features section of this document for more details.

Internet access is required during installation. This becomes optional once installation is completed. The EMS uses access to the internet to obtain information about FortiGuard engine and signature updates.

Endpoint Requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for Mac OS X

- FortiClient for Android OS
- FortiClient for iOS

FortiClient5.4.0 is supported, however, FortiClient 5.4.1 or later is recommended.

FortiClient is supported on multiple Microsoft Windows and Mac OS X platforms. The EMS supports all such platforms as endpoints.

Licensing and installation

For information on licensing and installing FortiClient EMS, see the *FortiClient EMS Administration Guide*.

Special Notices

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
  This document is available on the Fortinet Document Library on the FortiOS page.
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*
  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Main features

The core features of the FortiClient EMS 1.0.1 include the following:

CA Certificate Import from FortiGate

FortiClient EMS administrators can now import CA certificates from FortiGate with a click of a button and deploy it to its endpoints.

Email Alert Notifications

FortiClient EMS now supports email notifications to administrators for various alert conditions like zero-day malware detection, malware outbreak, C&C attack communication detection, and endpoint quarantine.

Vulnerability Scan Dashboard

A new Vulnerability Scan dashboard has been added to FortiClient EMS to provide visibility into the Vulnerability Status of all registered endpoints on the network. The dashboard displays the real-time status of all endpoint vulnerabilities and can be filtered based on severity and category.

FortiClient 5.4.1 or newer is required.

Upgrade

Upgrading from previous EMS versions

EMS 1.0.1 supports upgrading from EMS 1.0.

Downgrading to previous versions

Downgrading EMS 1.0.1 to previous EMS versions is not supported.

Resolved Issues

The following issues have been fixed in version 1.0.1.

Bug ID	Description
262374	FortiAnalyzer does not support FortiClient log upload if it is registered to EMS.
288121	Add option to configure the Vulnerability Scan feature in the Endpoint Profile GUI.
291532	Reboot prompt appears when installing the same package with EMS.
292695	Auto-connect VPN auto connects when EMS pushes any new profile.
292818	EMS scan request does not work with an offline device.
296094	FortiClient EMS is missing the Extended Sandbox feature.
300990	LDAPS does not choose correct certificate in the local store.
299300	FortiClient EMS is unable to add an installer.
303371	Add super user access for Windows and LDAP users.
300698	Multi-year license results in the wrong number of seats appended.
308773	*Server error 500* error occurs when more than nine on-net networks are added.
302088	Alerts/Events are not expandable to show all Alerts/Events.
299066	EMS uninstalls FortiClient successfully but GUI still shows that it is trying to uninstall.
356709	OpenSSL Security Advisory [1 March 2016].
366302	Unable to pop up an action on endpoint once FortiClient is uninstalled locally.
355396	Multiple instances of the same device on the EMS console.
373412	Typo in EMS endpoint profile.

Known Issues

The following issues have been identified in version 1.0.1. For inquires about a particular bug or to report a bug,please contact Customer Service & Support.

Bug ID	Description
290011	Error message may not appear. The write permission is denied in folder `FortiEMSInstaller`.
373350	EMS may not show failures when FortiClient unsuccessfully attempts to a apply patch for a found vulnerability.
369292	The notification server IP address, once configured on the EMS and used by numerous FortiClients, may not be configurable.
374164	When upgrading EMS through the *Upgrade Available* button, a completion message may not appear to the admin.
373827	EMS may not show endpoint compliance status.
282998	EMS may not support creating a Mac OS X Installer directly if the `FortiClientRepackager` is not used.

FORTINET®

High Performance Network Security